Description

Arrangement and method for coding and decoding digital data on the basis of the Internet Protocol

The Internet Engineering Task Force (IETF) is currently developing the next generation of the Internet Protocol (IP). The next generation of the Internet Protocol is called Version 6 of the Internet Protocol (IPv6). The Internet Protocol is a network layer protocol within the context of the OSI (Open Systems Interconnection) communication layer architecture. The Internet Protocol is the central element for linking various, autonomous communication networks to the worldwide Internet.

The format of the Internet Protocol is described in [1] for example.

An overview of Version 6 of the Internet Protocol (IPv6) can be found in [2].

Within the scope of the international work relating to IPv6, it is known practice to develop security extensions for the Internet Protocol. These security extensions, which can also be implemented within the scope of the currently up-to-date Version 4 of the Internet Protocol, are called IPsec. These are described in [3], for example.

The message format of the IPsec services uses the so-called IP Authentication Header, which is used to protect the integrity and authenticity of IP datagrams, and the so-called "IP Encapsulating Payload", which is used to protect the confidentiality and integrity of the data from higher protocol layers, e.g. the User Datagram Protocol (UDP) or the Transport Control Protocol (TCP), in so-called "transparent mode", or of entire IP datagrams, in so-called "tunnel mode".

The so-called OSI communication layers are described in detail in [4].

[5], [6], [7], [8] disclose so-called IPsec standards, in which two methods of allocating cryptographic keys are provided: within the context of so-called "Host Oriented Keying", all processes and users communicating between two terminals using IPv6 or using an IPv4 extended by IPsec use the same cryptographic key material. Within the context of so-called "User Oriented Keying", various users or processes on the two terminals communicating with one another can be allocated various cryptographic keys. In the case of IPv4, known transport system interfaces, for example Berkeley Sockets, Streams TLI, Winsockets, etc., are used for communication. However, so that applications, i.e. unspecified programs or processes, in relatively high network layers can use the novel security services of IPsec or else, generally, the new services of IPv6, extensions are currently being developed for the established transport system interfaces.

An Internet key management component (Internet Key Management Protocol, IKMP) and associated boundary conditions on the Internet are described in the form of so-called Internet Drafts in [9], [10], [11], [12], [13], [14], [15], [16] and [17].

However, one significant problem is that existing applications are not readily able to use the novel services provided by IPsec or by IPv6. To date, the novel services cannot be addressed without additional measures.

[1] discloses that the applications wishing to use the services of IPv6 and IPsec need to be matched to the new transport system interfaces by modifying

the applications. This document also discloses the practice of using configuration files for use for the new services. In this context, these configuration files are, in the first instance, static and, in the second instance, are component parts of the IPsec and IPv6 implementations. These configuration files inform a system with IPsec or IPv6 capability of the form in which it needs to provide transport services for an existing application without IPsec or IPv6 capability. In these two practices, however, a considerable disadvantage can be seen in that already existing applications cannot be modified in a general way, in view of the considerable quantity of existing applications. In addition, IPsec and IPv6 implementations do not support any interaction with applications or users.

The invention is based on the problem of specifying a method and an arrangement for coding digital data on the basis of the Internet Protocol and also a method and an arrangement for decoding digital data on the basis of the Internet Protocol which provide a simple means of enabling applications which were developed for an older version of the Internet Protocol to access the novel services of an Internet Protocol of the new generation.

The problem is solved by the arrangements and methods having the features based on the independent patent claims.

An arrangement for coding digital data on the basis of the Internet Protocol has a first means which is used to code the data on the basis of the format of a first Internet Protocol to give data having a first Internet Protocol format. In addition, a mapping unit is provided, which is used to map the data having the first Internet Protocol format onto data which can be processed by a second means, the second means being used to code the data on the basis of the format of a

second Internet Protocol to give data having a second Internet Protocol format.

On the basis of the arrangement for decoding digital data existing in a second Internet Protocol format on the basis of the Internet Protocol, a second means is provided which is used to decode the data on the basis of the format of a second Internet Protocol to give data having a decoded second Internet Protocol format. In addition, a mapping unit is provided, which is used to map the data having the decoded second Internet Protocol format onto data which can be processed by a first means, the first means being used to decode the data on the basis of the format of a first Internet Protocol to give the data.

In a method for coding digital data on the basis of the Internet Protocol, the data are coded on the basis of the format of a first Internet Protocol to give data having a first Internet Protocol format. The data having the first Internet Protocol format are mapped onto data which can be processed during further coding on the basis of a second Internet Protocol format. In a last step, the data are coded on the basis of the format of a second Internet Protocol to give data having a second Internet Protocol format.

In a method for decoding digital data existing in a second Internet Protocol format on the basis of the Internet Protocol, the data are decoded on the basis of the format of a second Internet Protocol to give data having a decoded second Internet Protocol format. In addition, the data having the decoded second Internet Protocol format are mapped onto data which can be processed during decoding on the basis of a first Internet Protocol format. The data are finally decoded on the basis of the format of a first Internet Protocol to give the data.

The arrangement and the method provide very simple means of permitting old applications which can use only the services of Internet Protocol Version 4

or older versions to use "IPsec or IPv6" as well. This means that the arrangement and the method make it possible for the new services offered by IPsec and IPv6, in general newer versions of the Internet Protocol, to be used with the "old" applications as well without the need to change the applications themselves.

The invention can clearly be seen in the addition, in the previous known architecture of the OSI communication layers, of an intermediate layer between the Internet Protocol layer (IP layer), which is also called network layer within the context of the OSI network architecture, of the "old" IPv4 and the "new" IPv6 or IPsec. This intermediate layer is used as a generic means in order to make future transport services of IPv6 available to applications which are based on the existing Version 4 of the Internet Protocol, and hence to assist the migration of said future transport services into the new network infrastructure.

This intermediate layer can be implemented and integrated both at application level and at operating system level. It is also possible to use this intermediate layer to provide a so-called proxy service.

Advantageous developments of the invention can be found in the dependent claims.

In one development, it is advantageous both for the arrangements and for the methods that the mapping unit has a parameter determination unit for determining parameters, and that, during mapping, additional parameters are determined which are necessary for coding the data having the first Internet Protocol format to give data in the second Internet Protocol format.

In addition, in one development, it is advantageous to design the parameter determination unit on the basis of at least one of the following types and to determine the parameters in one of the following ways:

- depending on the arrangement itself,
- depending on a user of the arrangement,
- depending on a process currently being carried out by the arrangement, or
- to determine the parameters from a database to which the arrangement has access, for example from a local database of the arrangement.

The figures show an illustrative embodiment of the invention, and this illustrative embodiment is explained in more detail below.

In the figures

Figure 1 shows a sketch of the arrangement for coding, transmitting and for decoding digital data;

Figure 2 shows a sketch of the procedure when mapping IPv4 applications onto data for IPv6 and IPsec.

Figure 1 shows a first arrangement 100 for coding digital data.

For the purposes of clear illustration, the OSI communication layers are used within the scope of the description below, these layers being described in detail in [4].

An application, preferably an application program which generates, on the basis of the Internet Protocol, digital data which are to be transmitted, is logically arranged in a so-called application layer 101.

So-called protocol data units (PDU) are exchanged between the individual layers. The individual PDUs 111 are uniquely associated with the individual layers.

Respective coding rules dependent on the respectively chosen known implementation of the layer are put into effect in the individual layers.

The respective layer can be implemented both in software and in hardware.

Within the scope of the arrangement, each layer is respectively in the form of a means used to implement the individual method steps on the basis of the communication protocol which is to be implemented in the respective layer.

The PDUs 111 of the application layer are supplied to a presentation layer 102.

After the PDU 111 from the application layer 101 has been processed on the basis of the rules of the presentation layer, a PDU 112 of the presentation layer 102 is supplied to a communication control layer 103.

After the PDU 112 of the presentation layer 102 has been processed on the basis of the protocol used in the communication control layer 103, a PDU 113 of the communication control layer is supplied to a transport layer 104.

The transport layer 104 preferably has the so-called transport control protocol (TCP) or else the user datagram protocol (UDP) implemented in it. After the PDU 113 from the communication control layer 103 has been encapsulated, the transport layer 104, i.e. the means used to implement the

transport layer, supplies a PDU 114 of the transport layer 104 to a network layer 105.

The network layer 105 usually has the Internet Protocol (IP), either in Version 4 or else in Version 6 or else in IPsec, implemented in it. Within the scope of the invention, a first Internet Protocol is implemented in the network layer, i.e. the data which are supplied to the network layer 105 in the form of the PDU 114 of the transport layer 104 are coded on the basis of the format of a first Internet Protocol (IPv4) to give data existing in a first Internet Protocol format.

The data having the first Internet Protocol format are supplied as PDU 115 of the network layer 105 to a mapping unit 106 used to implement an intermediate layer 106. The mapping unit 106 is used to map the data existing in the first Internet Protocol format 115 onto data which can be processed by a second means, a second network layer 107.

The data are supplied to the second network layer 107 in an intermediate layer PDU 116 in a format which the second network layer can process. In the second network layer 107, which is provided by a second means, the data are coded on the basis of the format of a second Internet Protocol (IPv6, IPsec) to give data existing in a second Internet Protocol format and are supplied to a data link layer 108 in the form of a PDU 117 having the second Internet Protocol format.

The data link layer 108 forms a PDU 118 of the data link layer 108 and supplies it to the physical connection layer 109.

The operations for mapping the PDU 115 from the network layer 105 in the intermediate layer 106 are explained in more detail below with the aid of figure 2.

One application based on Internet Protocol Version 4 201 usually uses existing transport system interfaces of IPv4, e.g. Berkeley Sockets or Streams TLI. The existing transport system interfaces 202 are provided entirely by the intermediate layer, i.e. the network layer 105 sees the mapping unit 106, i.e. the intermediate layer 106, as a data link layer.

The PDU 115 which has been adopted from the network layer 105 by the intermediate layer 106 is mapped onto the new transport system interfaces 203 of a second Internet Protocol (IPv6, IPsec). The new transport system interfaces 203 have dedicated security interfaces 204. Depending on the transport services provided in the second network layer 107, for example additional security services, additional parameters are required for coding on the basis of the second Internet Protocol format, in order to be able to use these services. An overview of various security parameters required within the context of IPsec and IPv6 are described in [4] in connection with the respectively provided methods for IPsec, IPv4 for the purpose of cryptographic data protection.

Within the context of this mapping, the invention also provides for the inclusion or integration of an Internet key management component (Internet Key Management Protocol, IKMP) 205 as described in [9], [10], [11], [12], [13], [14], [15], [16] and [17].

The coded data are transmitted in the form of data packets 112, containing the data in the second Internet Protocol

format, from the first arrangement 100 to a second arrangement 120 by means of a transmission unit 110.

The arrangements can be implemented both in software and in hardware, for example in a computer or else in a specific digital-electronic circuit matched to the task.

In the second arrangement 120, the data packets 112 are received and are supplied to a physical connection layer 121 of the second arrangement 120. After de-encapsulation on the basis of the protocol of the physical connection layer 121, a PDU 131 of the physical connection layer 121 is supplied to the data link layer 122 of the second arrangement 120.

After further de-encapsulation, i.e. decoding, in the data link layer 122, a PDU 132 of the data link layer 122 is supplied to the second network layer 123 of the second arrangement 120, in which de-encapsulation is performed on the basis of the second Internet Protocol format, i.e. on the basis of IPv6 or IPsec. Within the context of this decoding, by way of example, the cryptographic protection of the transmission is also implemented on the basis of IPv6 or IPsec.

The decoded data in the second protocol format are supplied as PDU 133 to the mapping unit 124, i.e. to the intermediate layer 124, and are in turn subjected to mapping. The mapping in the intermediate layer 124 is the inverse of the mapping in the intermediate layer 106 in the first arrangement 100.

The parameters required for processing can be determined in various ways. The parameter determination unit of the intermediate layer 106, 124 needs to be designed on the basis of the determination. The additionally required parameters may, by way of example, be configured on the basis of a specific output system, on the basis of a specific

user or else on the basis of a specific process. In this context, on the basis of a specific output system means depending on the respective arrangement used. On the basis of a specific user, in this context, means depending on the respective user currently using the arrangement. On the basis of a specific process, in this context, means depending on the process currently carried out by the arrangement.

Alternatively, the parameters can be requested from, by way of example, locally available security policy databases or general databases, or else can be determined interactively with a user of the arrangements.

After mapping in the intermediate layer 124, a PDU 134 is available which can be processed by the network layer 125, which is provided on the basis of the "old" Internet Protocol (IPv4). The PDU 134 of the intermediate layer 124 is supplied to the network layer 125, i.e. to the first means, and is decoded, i.e. de-encapsulated, on the basis of the first Internet Protocol format.

The result of de-encapsulation is that the network layer 125 forms a PDU 135 which is supplied to the transport layer 126. The transport layer 126 forms a PDU 136 which is supplied to the communication control layer 127.

The communication control layer 137 supplies a PDU 137 of the communication control layer 137 to the presentation layer 128. The presentation layer 128 forms a PDU 138 which is supplied to the application layer 129.

The double arrows in figure 1 indicate the bidirectional communication between the arrangements 100, 120.

The text below illustrates a few alternatives to the arrangements and methods described above.

Both the first arrangement 100 and the second arrangement 120 may also be provided independently, without the transmission medium, i.e. the transmission unit 110.

In addition, the transmission unit 110 can be understood such that any desired number of routers or bridges may be provided as switching units. The transmission unit 110 thus represents merely a logical channel between the first arrangement 100 and the second arrangement 120.

The invention can clearly be seen in the provision of an intermediate layer 106, 124 between the network layer used to provide the "old" Internet Protocol Version 4 and a second network layer, which is used to provide the "new" Internet Protocol (IPv6, IPsec), said intermediate layer being used to map the data formats of the IPv4 protocol format onto the IPv6 protocol format.

The following publications are cited in this document:

[1] R. Hinden, IP Next Generation Overview, Communications of the ACM, Vol. 39, No 6, pp. 61 - 71, June 1996

[2] D. Wagner, S. Bellovin, A "Bump in the Stack" Encryptor for MS-DOS Systems, in Proceedings of the Symposium on Network and Distributed System Security, San Diego, CA, pp. 155-160, February 1996

[3] RFC 1825, Security Architecture for the Internet Protocol, R. Atkinson, Network Working Group, pp. 1 - 22, August 1995

[4] A. Tanenbaum, Computer-Netzwerke [Computer Networks], Wolfram's Fachverlag, 2nd Edition, ISBN 3-925328-79-3, pp. 17 - 24, 1992

[5] R. Atkinson, RFC 1826, IP Authentication Header, August 1995

[6] R. Atkinson, RFC 1827, IP Encapsulating Security Payload, August 1995

[7] P. Metzger & W. Simpson, RFC 1828, IP Authentication using Keyed MD5, August 1995

[8] P. Karn, P. Metzger & W. Simpson, RFC 1829, The ESP DES-CBC Transform, August 1995

[9] T. Hardjono, B. Cain, N. Doraswamy, A Framework for Group Key Management for Multicast Security, July 98, available on the Internet on September 29, 1998 at the following address:

http://www.ietf.org/html.charters/ipsec-charter.html

[10] D. Piper, The Internet IP Security Domain of Interpretation for ISAKMP, July 7, 1998,

available on the Internet on September 29, 1998 at the following address:
http://www.ietf.org/html.charters/ipsec-charter.html

[11] D. Maughan, M. Schertler, M. Schneider, J. Turner, Internet Security Association and Key Management Protocol (ISAKMP), July 3, 1998
available on the Internet on September 29, 1998 at the following address:
http://www.ietf.org/html.charters/ipsec-charter.html

[12] D. Piper, A GSS-API Authentication Mode for ISAKMP/Oakley, December 18, 1997
available on the Internet on September 29, 1998 at the following address:
http://www.ietf.org/html.charters/ipsec-charter.html

[13] R. Pereira, S. Anand, B. Patel, The ISAKMP Configuration Method, May 13, 1998
available on the Internet on September 29, 1998 at the following address:
http://www.ietf.org/html.charters/ipsec-charter.html

[14] D. Harkins, D. Carrel, The Internet Key Exchange (IKE), June 1998
available on the Internet on September 29, 1998 at the following address:
http://www.ietf.org/html.charters/ipsec-charter.html

[15] B. V. Patel, M. Jeronimo, Revised SA negotiation mode for ISAKMP/Oakley, November, 1997
available on the Internet on September 29, 1998 at the following address:

http://www.ietf.org/html.charters/ipsec-charter.html

[16] R. Pereira, Extended Authentication Within ISAKMP/Oakley, May 13, 1998

available on the Internet on September 29, 1998 at the following address:
http://www.ietf.org/html.charters/ipsec-charter.html

[17] R. Thayer, PKI Requirements for IP Security, September 13, 1998
available on the Internet on September 29, 1998 at the following address:
http://www.ietf.org/html.charters/ipsec-charter.html